Laptops in Development:
A Survival Guide

David Cutting
dcutting [at] Purplepixie.org

Revision One, 26th May 2009

Introduction

Computers are increasingly important items used for both business and personal matters. It is increasingly common for development workers such as volunteers to take a laptop with them to their placements.

This laptop often becomes a very important tool for their work as well as critical for keeping in touch with those at home and for entertainment such as watching films or listening to music.

With good service and spare parts hard or perhaps impossible to come by it can be very difficult to get problems resolved. This guide is an attempt to provide some pointers on ways to protect your laptop from problems and to minimise the impact should problems occur.

Should there be anything you think is missed out from this guide please email the author as dcutting [at] purplepixie.org, all suggestions appreciated.

Physical Protection - Packaging

You can take all the steps in the world to protect against viruses but this won't protect against the laptop being dropped or damaged in-transit or in a later accident.

Most laptop bags provide some level of protection but are designed on the premise that you are taking care of the bag itself, for example not piling things on top.

When travelling by air or within developing countries by public transport this is often impossible to achieve. I have had to jump out of official government transport on various occasions to run to the back and beg people not to just dump the building supplies they have just picked up straight onto my laptop bag and its valuable contents.

It is a very good idea to keep something to wrap the laptop in where possible (I use a metre of so of bubble wrap brought with me from the UK) and also to have something between the screen and the keyboard so that if it does get squashed the keys aren't etched against the screen (I use the original piece of styrofoam that came with the laptop but have seen others with bits of cloth).

Physical Protection – Theft

Laptops are very desirable items and also unfortunately are exceedingly easy to wipe and reformat making them very attractive to thieves.

Gone are the days when in many countries nobody would know what was in that uniquely rectangular bag you had slung from your shoulder. In the world of today most people will know you're carrying a laptop or conversely if you're not carrying one then it is likely to be in your home.

This is the same as with any high-value items such as cameras.

You can lower this risk through basic security precautions and common-sense though you should always be prepared to loose the laptop if required (better that than your life if robbed) and have mitigated the effects of the loss (see Backups).

Always ensure you have the model details and crucially the **serial number** of your laptop stored in a safe place and maybe logged with someone at home as well.

In a recent incident in Namibia the police recovered laptops stolen from development workers within 12 hours of the theft but were only willing to return them on production of the serial numbers. The Peace Corp workers luckily had this information but their local colleague also targeted by the same thieves was not so lucky and has still not had theirs returned from police custody.

Physical Protection – Wear and Tear

Laptops by their mere definition as mobile devices get carted around, thrown about and exposed to all sorts of environments.

When used in development this can be more pronounced than back at home. You may use your laptop a lot more (in the UK I mainly used desktop machines for 90% of my work, here I use a desktop for well under 10% and my laptop the rest of the time) and the environment may be less conducive to good computer health (heat, humidity and above all dust).

It is important to keep your system clean and avoid working in overly humid or dusty conditions though this may sometimes be unavoidable.

Excessive dust can clog the air vents, affect fan performance, lead to overheating and, probably most commonly, cause optical (CD/DVD) drives to fail.

Always keep your laptop off with drives closed and covered when not in use. After use components retain static charge which will continue to attract dust given the chance.

Clean all CD/DVD media before use and if possible take with you an optical drive cleaning kit (see section on What to Take).

Viruses

Computer viruses are rife throughout the world and the developing world is no exception.

Whereas in countries with high internet connectivity the internet (poisoned web sites or emails) is the primary *infection vector* in countries with fewer internet connections it is the now ubiquitous USB memory sticks.

As the vast majority of computers in these countries do not have an internet connection they are unlikely to have any anti-virus software and those that do are not kept up-to-date.

It is highly likely that the majority of memory sticks handed to you by your colleagues (and your memory stick once returned from visiting a colleagues computer) will be infected by one or more viruses.

In some cases I have seen several hundred different infections on a single 512Mb stick.

However prevalent the problem though there are certain steps you can take which vastly reduce the chances of your laptop becoming infected.

At worse case though you may have to reformat your system and loose data. You should always ensure this will have the least possible effect (see Backups).

Use Anti-Virus and Keep it Updated

Always ensure you have a reputable anti-virus system installed and update it as often as possible from the internet.

Most anti-virus producers release daily updates covering all new forms of virus and making their system more effective at finding and deleting them.

There are a number of commercial products which offer time-bound updates and functionality (usually purchased in 12 month blocks) but there are also a number of products which are entirely free for personal use and offer, in this author's opinion, the same level of protection.

Where possible I would suggest avoiding the commercial brands which may well require a complex and expensive renewal part way through your placement.

Mac and Linux users: please note that you are not immune to viruses. It is commonly stated that there are no viruses affecting MacOS or Linux. This is incorrect though it is true they are very small in number and effectiveness. It is still recommended you install and keep up-to-date anti-virus software if for no other reason that you can cleanse memory sticks of viruses for your windows using colleagues.

Two free products for Microsoft Windows which are strongly recommended (only use one of them) are:

AVG Free Edition	http://free.grisoft.com
Avast Personal Edition	http://www.avast.com

Both of these also offer updated and more featured commercial (paid for) versions but the free version of each should be sufficient for most purposes.

For MacOS users:	**Clam XAV**	http://www.clamaxv.com
For Linux users:	**Clam AV**	http://www.clamav.net

Disable Auto-Run (Microsoft Windows)

Auto-Run is a feature within Microsoft Windows that allows removable media such as CD-ROMs and memory sticks to perform a specific action or run a particular program when they are inserted.

This was originally intended to be a useful part of Windows allowing a program installer to start automatically for example without the user having to specifically select it to run.

Unfortunately this functionality is often used by viruses and is the primary way viruses spread from media such as memory sticks and infect computers. When you plug the memory stick in the virus can be run automatically without any further action on your part.

Without auto-run you would (usually) have to specifically run the virus program for your computer to be infected.

Disabling auto-run will mean you loose the “What do you want to do with this device” popup when you put in a memory stick or CD but will also protect you against the majority of automatic virus infections.

How exactly to do this varies between versions of Windows, if in doubt google “disable autorun windows [your version]”.

Practice Safe Memory-Sticking

Even though you have disabled auto-run (or are not using Microsoft Windows) you should **always** scan a memory stick with your anti-virus program before opening it or any of the files contained upon it.

In Windows this is done by opening up “My Computer”, right-clicking on the memory stick device and selecting “Scan With [Anti-Virus Product Name]”.

Backups

If the worse should happen and your laptop is stolen, needs to be wiped or breaks completely it is crucial you have backed up your critical files.

Laptops can be replaced albeit at cost and inconvenience, that picture of the tribal festival or document you have spent the last year working on may not be replaceable.

It is always a good idea to backup your data and the more important to you it is then the more important it is that you back it up safely and securely.

When backing up consider what you want to keep. It is not necessary to backup the entire computer system, usually the vast majority of files are not personal to you and are linked to the operating system or application software installed.

Please note whichever methods you choose ensure you test the process of making the backup and as importantly recovering files from the backup.

Optical Media (CD/DVD)

The majority of laptops now feature a CD writer or DVD writer. Use of DVDs or CDs to backup your data is a great idea, they are usually cheap and readily available, can be read for use on any other computer system, are light and small so easily squirreled away.

If your computer has a writer drive it will probably have come with the software to write data discs (or it may be included in the operating system, Windows XP and later for example can write data CDs natively).

Using this method it is strongly recommended that you don't bother with or attempt to reuse discs given their cost, simply take regular backups that would duplicate what is already backed up along with any new information.

In this way even if your most recent backup is found to be corrupt or virus infected for example you will still have older copies to fall back upon.

Ensure that you do not store these backups with your laptop. I have heard of cases where backups are duly taken and stored in the laptop bag only to be stolen along with the laptop.

Memory Stick

Increasingly commonly available are large capacity memory sticks suitable for data backup purposes and these are gaining in popularity.

Be sure to distinguish between a memory stick you want to use for backups and one in everyday use. It will be not unlikely a memory stick in everyday use will become infected with a virus and may need to be wiped.

As with optical backup keep the backup media in a separate location to the laptop.

External Hard Drive

An external hard drive is a USB connected drive offering significant storage. Many development workers now use these to store additional information such as films or music as well as a backup copy of their information.

The same constraints as with a memory stick should be applied and additionally the fact it contains moving parts and is susceptible to environmental problems should be considered.

Online Storage

If you are lucky enough to enjoy access to a reliable high-speed internet connection then you could consider online backup and storage of data onto the internet.

There are a number of commercial services available but you may find free services such as Google Documents (http://docs.google.com) suffice.

You may also choose to simply email yourself copies of important files to an email provider that stores data indefinitely online such as Google Mail (http://mail.google.com).

As internet connectivity in countries this will become a more common form of backup.

Recovery Media

Regardless of how well you look after your system there may well come a time when you need to reformat and reinstall the operating system. This might be the result of a virus or other software corruption or perhaps following a hard drive crash and replacement.

Most modern laptops do not come with an operating system disc (a CD or DVD containing a copy of the operating system e.g. Microsoft Windows).

Instead the laptop will have a *hidden recovery partition* taking up part of the hard drive storage.

How precisely you start this recovery process varies from model to model (make sure you know before you travel, it should be in the instructions or on the manufacturer's website).

Because a number of catastrophic failures can affect this recovery partition most laptops will provide you the option to burn a set of recovery discs (CDs or DVDs) which can be used in-lieu of the recovery partition to restore the system.

Again the precise instructions vary from model to model.

You should make sure that you burn a set of these discs and keep them in a safe place.

If you have a full set of recovery discs and a full backup of your data even a total virus infestation is no more troublesome than an hour or so of reformatting your laptop with the recovery discs and then restoring your data from backup.

Battery Life

Laptops have a variety of battery lives from under an hour (large desktop replacements) to in excess of eight hours (some netbooks).

Commonly this battery life will decrease during the life of the laptop.

Generally it is a good idea to use the battery every so often (don't simply always use the mains adaptor) to keep the battery in good health.

You should also read and adhere to any instructions that came with your laptop on care of the battery which may include some additional steps to prolong the longevity and life of the battery.

What to Take

- Your laptop (obviously)
- A copy of the make/model and serial number
- A copy of your warranty document (if applicable)
- Protection for transit to country and when in-country (e.g. bubblewrap)
- Something to protect the screen from the keyboard (e.g. styrofoam sheet)
- Recovery media (to restore laptop)
- Blank media (CD, DVD, memory stick or hard drive) for backups
- Anti-virus software you are happy to use and keep updated
- Any discs associated with devices you wish to use such as cameras in case you need to reinstall

You may also like to consider taking the following which are liable to be hard to come across in-country or very expensive to import:

- Spare battery
- Spare mains adaptor